2007-09
Identity Assurance

Introduction:

Assuring that identified individuals and things are as they are portrayed is fundamental to most security processes. As a result, the conceptual need for identity assurance is indeed great. But the reality of assured identity is far more complex.

The identity life cycle

To get a clear handle on identity assurance, you have to understand the life cycle of the person or thing you are identifying. For people, for now, it can be reasonably assumed that, at birth, they have no predilection to be more or less worthy of trust. While physiological traits of individuals may lead to neurological limitations on what they will or will not do, the tracking of individuals from the womb to the tomb may be necessary in order to gain clarity around their worthiness for trust, assuming that the level of trust placed in them is high enough to justify the scrutiny.

For most enterprises concerned about human identity, the process begins with an authentication performed by the HR department that associates the purported identity with government documents. A driver's license or a passport is usually accepted, and a second form of photographic identification is used for more certainty. But at the end of the day, few enterprises go further that a minimal background criminal records check or verify that the person present is the actual person associated with the identifier. As the worker works for longer periods of time, the enterprise gathers more history of competence and their ability to work well with others and the level of personal trust increases. This is unavoidable for small companies or small longstanding groups within larger companies, but it breaks down both because being personable and friendly are improperly associated with trust and because large enterprises rarely have enough ongoing contact between individuals to develop these sorts of trust bonds for everyone who is involved in doing tasks mandating levels of trust. Of course this trust relationship does not usually go two ways. The worker usually has no way to determine whether the employer is trustworthy or who they claim to be except by the history of getting paid, and the systems and facilities they access do not demonstrate themselves to be legitimate to the worker in most cases.

Assuming that we know what why we trust people or other actors and how far, we still have to authenticate them to be certain that we are trusting the real actor.

Life cycle authentication?

The second part of identity assurance is being able to prove that the actor asserting an identity is indeed the individual being asserted. Whether is is a person or a system, there are physical characteristics that can be used to demonstrate tho or what they are. But these biometrics (or in the case of things, mechano-metrics or electro-metrics) are just that; metrics. They are things that can be measured and, to within a defined degree of certainty, demonstrate their authenticity. The degree of certainty is the key issue here, because, they are the mechanisms that provide part of the assurance that they are what or who they claim to be. The cost of these devices is going down. For example, for about $5 per reader, magnetic stripe cards can be authenticated to an increased extent. However, don't be fooled by the devices and the technical prowess with which they have been implemented. There are two basic problems remaining; any security mechanism can eventually be defeated, and in the case of these metrics they cannot be replaced like a password can be - it's just a matter of the cost and time.

But the second problem is far harder to address. That's the problem of assuring the life cycle of the association of authentication information to the individuals and their metrics. If a single data entry clerk is replaced, has their children held hostage, or is otherwise corrupted, they can alter the process for many individuals. If someone who is highly trusted has their biometrics forged, or if we alter the biometrics prior to initial registration, the system falls apart. If an authentication is circumvented, then all of the devices that depend on it become less sure. If the system is made unavailable for a period of time, all of the systems that depend on it for operational continuity may be disabled, or revocation of credentials may be disrupted for a period. As we pile more trust on these authentications, a single breech becomes far more damaging. And even something like a computer virus has the potential to tailgate on top of all of the authentications used by all of the users using infected systems to gain their combined authority.

Conclusions:

Identity assurance it vitally important to proper operations of trust within information and other infrastructures as well as in a wide array of other human and automated activities. It is a hard problem and improvements in identity assurance are very beneficial. But at the same time, these improvements may lead to a false sense of security. Clearly, the challenge has to be met with increasing rigor as we increase the use and dependence on more and more centralized identity assurance.

Fraud of the month

Every month, we take an example from "*Frauds Spies and Lies and How to Defeat Them*" and describe a recent example. From page 34-35:

"Phantom employee"

> *"...an employee who gets paid but doesn't actually exist..."*

Variations on this have been used to penetrate even the highest security facilities and the most critical elements of national infrastructure. But they work well for all sorts of attacks, particularly attacks on the identify assurance system. If the employee who first enrolls has reproducible prosthetic fingerprints, and if fingerprints are used as a biometric authenticator, a replacement can be authenticated wherever needed by providing them with the same false biometrics.

Page 179, "Employee Frauds" provides a host of approaches to reducing the phantom employee challenge including:

> *Background checks and audits, qualifications checks, working hour audits, manager review and investigation, and better background checks.*

But at the end of the day, you can only go so far before you have to trust, and if history tells us anything, the only solution to excessive trust is to diffuse risk by disaggregating it.

Chet's Corner

I am Chet... I am... OK – I'm not Chet. But at the same time, I am. What's in a name after all? If you prick me do I not squeal? But suppose I'm not Chet. How could you tell? You could ask me, but then you would have to believe that the Chet you asked is the same Chet you thought you were asking. And is the Chet you think you know really the Chet you think you think you know? And if I'm not Chet, who am I? And who are you to even ask if I am who I say I am? If I am trying to lie, why would I tell you the truth? OK – now I am really confused. Who am I supposed to be?

"Always look on the bright side of life"!

Service Summary

Every month we feature one of our services and give an example of how it benefited one of our clients. This month it's our in-depth custom research.

Most firms in the information security business do what we would call standard security consulting. They do work with checklists and common practices that, while they don't work really well, often succeed. We are not most firms. We always bring true expertise, and those same experts also do the in-depth custom leading edge research that goes beyond the current state of the art to develop new knowledge that is sorely needed. In one recent example, for a forensics client, we were asked to extract data from a floppy disk that nobody else could fully read and authenticate the data we read in court.

The little bit of research involved in reading the disk was not really leading edge. But to make sure the data we got was right, we had to apply advanced mathematics and solve coding problems that had never before been solved. We had to determine that multiple errors hadn't combined to overcome the coding system used on the disk, and we had to analyze the errors produced only by reduction of electromagnetic flux density in writing and reading of floppy disks. As it turned out, there were no prior publications in this area and the work we did meets standards for a refereed journal article.

Not every client needs a breakthrough to meet their protection needs, but for those that do, it's good to know that we're here to help.

Mollie gets the last word in

My Chilean identity card didn't get processed correctly. The finger print process was fouled up and, as a result, I had to wait an extra two weeks before I could go places and see things that everyone else was already going and seeing. The national identity card system in Chile can't even take finger prints reliably and process them through the system. I think it was because I didn't act like I would go out with the man who took the prints and interviewed me when I first arrived. When people tell me that a national ID card will help me, I tell them that it will only work if it doesn't turn into a dating service for the workers.